(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80078 A1

(51) International Patent Classification[7]: G06F 17/30, 17/00

(21) International Application Number: PCT/US01/10606

(22) International Filing Date: 2 April 2001 (02.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/197,620	14 April 2000 (14.04.2000)	US
09/618,145	11 July 2000 (11.07.2000)	US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:

US	60/197,620 (CON)
Filed on	14 April 2000 (14.04.2000)
US	09/618,145 (CON)
Filed on	11 July 2000 (11.07.2000)

(71) Applicant and
(72) Inventor: MEISEL, William, S. [US/US]; 18740 Paseo Nuevo Drive, Tarzana, CA 91356 (US).

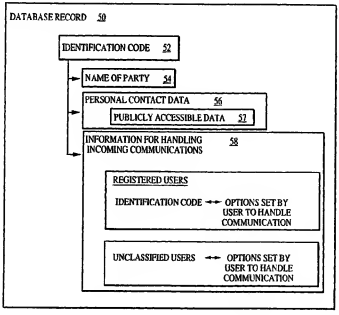
(74) Agent: BORODACH, Samuel; Fish & Richardson P.C., Suite 2800, 45 Rockefeller Plaza, New York, NY 10111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: HANDLING AND MANAGEMENT OF COMMUNICATIONS



(57) Abstract: A communication system (10) includes a database (12) storing an identification code (52) in a database record (50). Each identification code (52) is associated with a respective party (54) and is independent of a particular type of communication medium. The database (12) also stores information including options (58) set by a first party (54) indicative to how communications addressed to the first party (54) is to be handled. Service provider equipment is configured to automatically handle a communication intended for a party (54) according to the instructions (58) set by the party.

WO 01/80078 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

HANDLING AND MANAGEMENT OF COMMUNICATIONS

BACKGROUND

The invention relates generally to the handling and management of communications.

Various types of communication exist including telephone, electronic mail (email), facsimile (fax), paging, specialized wireless communications (such as Personal Digital Assistants), postal mail, and instant messaging. Managing the different types of communications has become increasingly complex for individuals as well as companies and organizations. For example, individuals may have multiple versions of a given type of communication, such as both business and home email addresses, as well as home, business, and wireless telephone numbers. Furthermore, the types of communications are becoming less distinct. Callers can retrieve email messages by telephone by having the messages read to them using text-to-speech synthesis, and can reply by voice. The reply voice messages may, in some implementations, be sent as an audio file attachment to an email message.

An additional complicating factor in managing communications is the receipt of unsolicited messages, sometimes called "junk mail" or "spam." Handling such undesirable communications can be time-consuming. Further-more, changes to telephone numbers, email addresses and other addresses have become increasingly common. For example, a telephone number may change as a result of a change to an area code. Similarly, an email address may change when one switches to a different service provider. Such changes make it inconvenient and difficult to ensure that all parties with whom one would like to be able to communicate are notified of the address changes in a timely manner.

Therefore, it would be desirable to provide techniques that facilitate and improve the handling and management of communications over various media.

SUMMARY

In general, a communications system includes a database storing identification codes each of which is associated with a respective party and is independent of a

particular type of communication medium. The database also stores information including options set by a first party indicative of how communications addressed to the first party are to be handled. The system includes service provider equipment configured to intercept a communication from a sender, to query the database for instructions regarding handling of the communication based on an identification code associated with an intended recipient of the communications, and to automatically handle the communications in accordance with the instructions.

Methods of use and articles that include a computer-readable medium with computer-executable instructions also are disclosed.

Various implementations may include one or more of the following features or advantages. The techniques described here can facilitate and improve the handling and management of communications over various media. In particular, a party can dictate how incoming communications addressed to that party are to be handled. Options can be set for handling communications from specific parties as well as unclassified parties. The techniques allow the options to be changed readily. Moreover, by providing a single identification code to each party for use in sending messages over any one of multiple communication media, each party can more easily control when, how and where it receives the communications addressed to it.

Additional features and advantages will be readily apparent from the following detailed description, the accompanying drawings and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an exemplary communications system including a database according to the invention.

FIG. 2 illustrates the structure of an exemplary record stored in the database.

FIG. 3 is a flow chart of a method for handling a communications according to the invention.

FIG. 4 is a flow chart of a method by which a party can become a registered user of another party.

FIG. 5 illustrates various security features according to one implementation of the database.

FIG. 6 illustrates the system of FIG. 1 with the addition of a mirrored database.

DETAILED DESCRIPTION

FIG. 1 illustrates an exemplary communications system 10 that includes a central database 12. The database 12 stores a record 50 (FIG. 2), including a unique communications identification code 52, for each party that is enrolled in the system 10. The identity of the party 54 associated with each particular code also is stored in the database 12.

The identification codes can take the form of alphanumeric strings. In some implementations, the codes may consist only of numbers so that they easily can be entered on keypads or spoken and recognized accurately with automatic speech recognition equipment. The strings of numbers preferably have internal relationships such as check-sums, that allow the codes to be validated, thereby facilitating detection of fraudulent numbers. The codes should be long enough so that they can provide unique identifiers for a large number of people. Also, the number of valid codes can be limited to a small fraction of the possible codes to reduce the likelihood that guessing a number randomly will generate a valid code. In some implementations, a party also can choose an alphanumeric alias that is not in use and that can be used as a shortened version of the identification code when a full keyboard is available. Optionally, when entered on a telephone or similar keypad, alphanumeric codes can be translated into corresponding numeric codes. To avoid conflicts when entering identification codes this way, alphanumeric codes can be generated so that they are unique even when entered on a telephone or similar keypad using the letters on the keypad for the letters in the code.

Additional information associated with a particular identification code can be stored in the database 12 as well. The additional information stored in the database 12 can include personal contact data 56 that can serve as an electronic business card. In addition, the personal contact data 56 can include other information, such as a link to an Internet Web site or a photograph of the person.

In general, a party can enter additional information 58 into the database 12 by setting various options that allow the database automatically to manage incoming communications addressed to that party. Thus, a party can block all communications for which the sender does not provide its identification code or the party may choose to block all communications from a particular source identified, for example, by a communications identification code or email address. Alternatively, communications from a particular source can be categorized by priority so that communications having different priorities are handled differently. Thus, high priority phone calls might be forwarded to a wireless phone, while lower priority calls might be forwarded to a message center. Similarly, business emails might be forwarded to a business email address, while personal emails might be forwarded to a personal email address. In addition, the type of access allowed by a particular source can be controlled. For example, a party might choose to receive communications from a particular source only email. Other options can be selected and stored by the database 12.

When a party applies for an identification code, the party provides personal contact data and sets basic options related to the handling and management of incoming communications addressed to that party. Preferably, the identity of the party should be verified and each party should be assigned only a single identification code. In one implementation, the personal information provided by the applicant can be validated, at least partially. For example, the applicant's identification code can be sent by postal service to the mailing address specified by the applicant with a request that the applicant confirm receipt in order to activate the applicant's code. Alternatively, the applicant's identification code can be sent to the email address specified by the applicant with a request that the applicant send a reply. If no reply is received within a specified period, the validation would fail.

The personal contact data can include data 57 that is publicly available to other parties who are given permission to access the database 12. Such publicly accessible data can include the full name of the party, its mailing address, telephone number or email address, as well as other information. If, for example, party A gives its identification code to party B, then party B can access the publicly available data 57 associated with party A through a personal computer 14 or other device connected

to a network 16 such as the Internet. Software residing, for example, on the personal computer 14 allows party B to use the computer to enter the identification code of party A and access the publicly available data associated with party A. Preferably, once the identification code of party A is entered and transmitted to the database 12, the publicly available data 57 automatically is retrieved and saved locally in the computer 14 or other device, thereby avoiding typing errors.

As further shown in FIG. 1, communications through the system 10 can use one of several types of communication. For example, the system 10 can include a telephone service provider 18 that allows a party to send communications from the personal computer 14 or other device through a telephone connection 22 over a telephone line 20. The system also can include an email service provider 24 that allows a party to send communications from the personal computer 14 or other device through a network connection 22 over a network 20 such as the Internet. Other communications service providers, such as facsimile service, automated postal service and instant messaging, also can be used in the system 10. Similarly, other devices, including personal digital assistants (PDAs) or enhanced telephones, can be used instead of the personal computer 14.

In general, as shown in FIG. 3, when sending a communication through the system 10, the identification code associated with the intended recipient is included 60 as part of the communication. In various implementations, the sender and recipient's respective identification codes can be entered either manually or automatically.

Manually entering the identification codes can include the following. For telephone communications, the recipient's identification code can be entered using a telephone keypad. Alternatively, the recipient's code can be spoken into the telephone receiver and recognized using speech recognition techniques. For email communications, the recipient's code can be included in the "to" field. Alternatively, the recipient's code can be included in the body of the email message and indicated by a marker or simply recognized by context. The recipient's identification code also can be used in other forms of communication, including instant messaging and standard postal service. For example, with respect to standard postal mail, the

recipient's identification code can be included in the mailing address and the sender's identification code can be included in the return address. The codes can be incorporated, for example, into an automated mail system that uses bar codes. Similarly, in the context of an instant messaging system, the sender and recipient's codes can be associated with the system's identifying "handles."

In some situations, a specific device such as a personal computer or wireless telephone can be associated with a particular sender so that the sender's identification code automatically is incorporated as part of the communication prior to transmittal. In yet other implementations, the sender or recipient's identification code can be entered automatically in response to the entry of corresponding information. In one example, a sender of a voice communication by telephone would speak the name of the recipient into the telephone receiver to initiate the communication. The recipient's identification code would automatically be retrieved from a directory and placed into the communication. The sender's core can similarly be added.

As further indicated by FIG. 3, a communication sent through the system 10 is intercepted 62, for example, by the appropriate service provider 18, 24. The recipient's identification code is extracted 64 from the intercepted communication. If the sender's identification code is not included in the communication, then the communication is treated 66 as originating from an unclassified sender. Assuming that the sender's identification code is included in the communication, it too is extracted 68. Control software uses the sender and recipient's identification codes to query the database 12 and check 70 whether the sender is listed as a registered user with respect to the recipient. FIG. 4, discussed below, illustrates how one party can become a registered user of another party. If the sender is not a registered user of the recipient, then the communication is treated 72 as originating from an unclassified sender. On the other hand, if the sender is listed as a registered user of the recipient, then the communication is handled 74 in accordance with the options previously set by the recipient and stored in the database 12 for communications originating from the particular sender. Communications from unclassified senders are handled in accordance with options previously set by the recipient or in accordance with default options stored in the database 12.

In the implementation illustrated in FIG. 1, each service provider 18, 24 runs software to handle management of communications based on information stored in the database 12. In such a distributed scenario, the service providers 18, 24 can utilize the database 12 as an information resource or can form part of a forwarding service of the database itself. Communications between the service provider 18 and the database 12 can take place over a network 30. Similarly, communications between the service provider 24 and the database 12 can take place over a network 32. The networks 30, 32 can be implemented, for example, using the Internet. In other implementations, software for handling management of communications can reside locally at the receiving end of the communication, for example, in the recipient's personal computer 14A for email or telephony, or in a PBX voice-mail system for telephone calls.

Handling of a particular communication can include one or more of the following exemplary actions depending on the options previously set by the recipient and stored in the database 12. The control instructions as dictated by the options selected by the intended recipient and stored in the database 12 can indicate that communications from unclassified senders should be treated, for example, as low-priority messages or simply rejected.

Some communications may be rejected if the intended recipient sets options to block all communications from the sender or communications sent by the sender over a particular communications medium. In such situations, the content of the communication can be saved in the database 12 for a specified period in case the recipient wishes to recover or review rejected messages.

In some situations, the recipient's instructions as indicated by the options set and stored in the database 12 may require changing the form of a message. For example, a recipient may want voice messages from a particular party to be delivered as attachments to an email message. In other cases, the recipient may want email messages to be communicated over the telephone using text-to-speech synthesis. Technology for performing such text-to-speech synthesis is available commercially.

In some cases, existing features of the message type are used. Thus, some email systems are capable of attaching an indication of priority to the communication.

and some email programs handle different priorities differently, for example, by storing them in different electronic folders and/or highlighting high priority messages. Existing telephone systems can put a call through or put it into a voice mail queue. Some systems allow high-priority queues. The options selected by the recipient and stored in the database 12 can indicate, for example, that for high-priority messages or messages from specific individuals, the recipient should be paged or called on a mobile phone.

If there are multiple addresses for the message type, for example, if there are multiple phone numbers, the options set by the recipient can indicate where messages from the sender should be directed.

In other situations, control instructions stored in the database 12 may indicate whether the sender is to be informed of the disposition of the message. For example, the options set by the intended recipient may indicate that a reply should be sent to a party whose message was rejected indicating that the message was undeliverable. For high-priority messages, the options set by the recipient may dictate that the sender should receive a courtesy reply that the message was received and that a substantive reply can be expected soon.

FIG. 4 illustrates one technique by which a party, such as party C, can become a registered user of another party, such as party D. Initially, party C provides 80 its identification code to party D along with a request to become a registered user. Party D then can access the database 12, for example, over the network 16. Using party C's identification code, party D can review the publicly available data about party C that is stored in the database 12. Based on the publicly available data about party C and other known information, Party D decides 82 whether to list party C as one of its registered users. If party D decides to accept party C as a registered user, then party D would select and set 84 various options indicating how communications from party C are to be handled. The database 12 automatically can send 86 a communication to party C indicating that party C is now a registered user of party D. The communication to party C also can disclose the identification code of party D and can indicate what forms of communication are acceptable for messages sent by party C to party D.

If party D declines to accept communications from party C, one of several actions can be taken. In one scenario, party D can simply ignore the request of party C. In that case, party C would not receive any message indicating that party D does not wish to receive communications from it. Communications from party C, however, are effectively blocked. Alternatively, party D may select and set 88 options in the database 12 to block all messages from party C. The database 12 automatically can send 90 a message to party C indicating that its request was not accepted. Depending on the options set by party D, party C may be able to appeal party D's decision not to accept its communications. However, party D's identification code would not be provided to party C.

The database 12 should be secure from undesirable outside intrusion. FIG. 5 illustrates an exemplary implementation. As shown in FIG. 5, there are two physical layers 92, 94 of security. Outside inquiries over the networks 16, 30, 32 initially are handled by servers 90 in the secondary layer 94 of security. The servers 90 can receive outside requests for contact or control information and transmit the requests over a secure encrypted line to the database 12. Another server 100 processes requests directed to the database 12 from the servers 90 and forward the requests to the database 12. The database 12 returns an encrypted reply that can be decoded within one of the secure servers 90 and can be sent to the processing application. The encrypted version then can be erased from the disk in the server 90. Thus, the servers 90 need not have a significant amount of data at any given time. Furthermore, the data in the servers 90 is constantly changing. Even if an intruder penetrates the protection on the servers 90, he would not have access to the database 12. Other software protection in the database 12 can include processing only very specific types of requests in highly structured software that is designed to avoid hacking. In addition, firewall software can be provided to protect the database 12 and the servers 90 separately. The physical security can protect the servers 90 from access by parties that are not authorized personnel.

In addition to the database 12 and an associated archive 96 for storing backup data and changes to the database contents, one or more mirror encrypted databases 98 can be included to provide additional reliability. As shown in FIG. 6, a mirror

encrypted database 98 that includes the contents of the database 12 can serve as a local database for one or more service providers, such as the provider 18.

Certain information contained in the database 12 can be modified by the user. For example, a user can update its personal contact data 56, including the personal data 57 that is available to the public. In addition, a user can change the way in which the system is set to handle communications addressed to the user. Such changes can be made by accessing the database 12, for example, from the personal computer 14A or other device and changing the settings for the options 58 for handling incoming communications from either registered or unclassified users. To prevent changes being made by unauthorized persons, each enrolled user may be required to use a private password to obtain access and make changes to its information stored in the database 12. In some implementations, old personal contact data is stored in the archive 96 (FIG. 5). A user can set options using the database 12 so that changes to the user's personal contact data automatically are communicated to parties that previously have communicated with the user.

Changes to a party's identification code may occur for one of several reasons, and a user can request that its identification code be changed at any time. For example, if a user is receiving an excessive number of communications from telemarketing companies, the user may wish to obtain a new identification code. The party with whom the new identification code is associated can specify a list of other parties who are to be informed of the new identification code automatically. The database 12 then can transmit a message to inform the other parties of the new identification code.

Expired identification codes also can be retained in the database 12 or the associated archive 96. The expired and new identification codes can be linked to allow the user to set options that determine how communications addressed to an expired identification code are to be handled. In one implementation, communications addressed to an expired identification code are treated as originating from an unclassified sender. Optionally, the sender of the communication automatically can be informed of the new identification code. In other implementations, communications from a sender who directs the communications to

an expired identification code can be treated in the same way as communications from that sender were previously handled. The sender can be notified of the new identification code automatically. After a specified number of such notifications, if the sender does not begin using the new identification code, communications from that sender are handled as originating from an unclassified sender. Combinations of those techniques can be used as well.

Software installed on the user's personal computer 14A can cause the computer to retain the identification codes of contacts with whom a party has previously communicated. The list of identification codes for such contacts can be stored, for example, in a database in the user's personal computer 14A or other access device. The software also can cause the computer 14A to poll the database 12 periodically and obtain up-to-date changes to identification codes of other parties with whom the user has communicated. Similarly, software can cause the computer 14A to poll the database 12 and obtain up-to-date changes to personal contact data of other parties with whom the user has communicated. Any changes can be obtained and stored automatically in the user's personal computer 14A or other access device on a periodic basis so that the list of contacts stored in the personal computer is current.

If a sender contacts a recipient using an identification code that differs from the code used in an earlier communication, the system automatically can check whether other identification codes have been issued to that sender. If such an identification code has been issued to the same sender, the database 12 can handle the present communication in the same way as dictated by the earlier identification code. Parties can be discouraged from improperly obtaining an identification code by pretending to be another party because of costs and other controls, including the ability of a recipient to protest a call to the organization maintaining the database 12.

In some implementations, a communication that is a reply to an earlier communication can be handled in the same manner as the original message, in other words, according to options set by the addressee of the reply message. In other case, replies can be handled differently from unsolicited communications. For example, a software flag or other label can be inserted into the reply automatically. The database

12 can be configured to recognize such a label and to automatically pass the reply back to the sender of the original communication.

The database 12 also can be configured to compile and retain lists of the recipient identification codes accessed by each sender. Broadcast communications, such as advertising, can be detected automatically by detecting overuse of an identification code by a transmitting party. Such identification codes can be placed on a list of broadcasters, and parties enrolling in the system can elect to reject messages from anyone on the broadcaster list. To prevent broadcasters from obtaining additional identification codes, multiple identification codes assigned to a single party can be correlated to one another. New identification codes assigned to the party automatically can be placed on the broadcast list. An appeals process can handle exceptions. Broadcasts of changes of contact information that are initiated by the database 12 need not be considered broadcasts for this purpose.

Similarly, if a party attempts to initiate numerous communications using invalid identification codes within a short period of time, that party's access to the database's services may be terminated.

In some implementations, the database 12 can be supplemented by associated services that handle various communication types as well as provide contact and control information. Such associated services can include, for example, an email forwarding service that uses information in the database 12 to control the disposition of the email based on the sender. The types of control can include rejecting specified email messages, categorizing email messages by priority, and directing the email to different email accounts based on control instructions in the database 12. In another implementation, a forwarding service for standard postal mail can include screening out unwanted mail or delivering it in a separate container, under control of the database 12. The mail can be delivered in other forms, for example, by scanning it into a digital form to be viewed by a browser or similar software. The foregoing services need not be located at the site of the database 12, but can use the database remotely.

The techniques described here can be implemented in hardware and/or software. In one implementation, a dedicated processor includes instructions for

performing the functions described above. Alternatively, the system can include a general-purpose processor. Computer-executable instructions for implementing the techniques can be stored as encoded information on a computer-readable medium such as a magnetic floppy disk, magnetic tape, or compact disc read only memory (CD-ROM).

Other implementations are within the scope of the following claims.

What is claimed is:

1. A communications system comprising:

a database storing identification codes each of which is associated with a respective party and is independent of a particular type of communication medium, and further storing information including options set by a first party indicative of how communications addressed to the first party are to be handled; and

service provider equipment configured to intercept a communication from a sender, to query the database for instructions regarding handling of the communication based on an identification code associated with an intended recipient of the communication, and to automatically handle the communication in accordance with the instructions.

2. The communications system of claim 1 wherein the first party can remotely access the database to set options that are stored in the database and that are indicative of how a communication from a second party that is addressed to the first party is to be handled based on an identification code associated with the second party and included as part of the communication from the second party.

3. The communications system of claim 1 wherein the database includes options that can be set by the first party to indicate whether a communication from a second party that is addressed to the first party is to be delivered or blocked based on an identification code associated with the second party and included as part of the communication from the second party.

4. The communications system of claim 1 wherein the database includes options that can be set by the first party to indicate that communications addressed to the first party from a second party are to be delivered only if the communications use selected communication media.

5. The communications system of claim 1 wherein the database includes options that can be set by the first party to indicate that communications addressed to the first party from a second party are to be delivered over a specified communication medium, wherein the service provider equipment is configured to reformat such communications for delivery over the specified medium and to deliver the communications to the first party via the specified medium.

6. The communications system of claim 1 wherein the database stores personal contact data associated with each party, wherein a particular party can remotely access the database to review the personal contact data associated with another party.

7. A method of processing a communication, the method comprising:

extracting a first identification code from the communication, wherein the first identification code is associated with an intended recipient of the communication and is independent of a particular type of communication medium;

querying a central database for instructions regarding handling of the communication based on the identification code associated with the intended recipient, wherein the instructions are based on options previously set by the intended recipient; and

automatically handling the communication in accordance with the instructions.

8. The method of claim 7 including:

extracting a second identification code from the communication, wherein the second identification code is associated with a sender of the communication and is independent of a particular type of communication medium;

wherein the instructions are based on both the first and second identification codes.

9. The method of claim 8 wherein the instructions are based on options previously set by the intended recipient for handling communications from the sender.

10. The method of claim 9 including preventing delivery of the communication if the instructions indicate that all communications addressed to the intended recipient from the sender are to be blocked.

11. The method of claim 10 including storing the content of the undelivered communication for a specified period to allow subsequent retrieval by the intended recipient.

12. The method of claim 9 including preventing delivery of the communication if the instructions indicate that communications addressed to the intended recipient from the sender are to be delivered only if the communications are transmitted over one of selected group of communication media and if the communication is not sent over one of the selected media.

13. The method of claim 9 including reformatting the communication for delivery over a specified medium and delivering the communication to the intended recipient via the specified medium if the instructions indicate that communications addressed to the intended recipient from the sender are to be delivered over the specified communication medium.

14. The method of claim 9 wherein the communication includes an indication of the communication's priority, and wherein the instructions are based on options previously set by the intended recipient for handling communications from the sender depending on the priority associated with the communication.

15. The method of claim 8 including automatically inserting the second identification code into the communication in response to the entry of corresponding information by the sender.

16. The method of claim 7 including:

detecting communications that are broadcast;

storing a list of identification codes of parties broadcasting messages; and

handling messages from a party on the list and addressed to the intended recipient in accordance with instructions based on options previously set by the intended recipient with respect to messages originating from parties on the list.

17. The method of claim 7 including:

extracting a second identification code from the communication, wherein the second identification code is associated with a particular sender of the communication and is independent of a particular type of communication medium;

determining whether the intended recipient has previously set options indicating how communications from the particular sender are to be handled; and

handling the communication as having been sent by an unclassified sender, if the intended recipient has not set options indicating how communications from the particular sender are to be handled.

18. The method of claim 17 including handling the communication in accordance with instructions based on options previously set by the intended recipient for handling communications from unclassified senders.

19. The method of claim 7 further including:

storing a new identification code associated with the intended recipient; and

automatically informing other parties with whom the intended recipient has previously communicated about the new identification code.

20. The method of claim 19 including:

linking the new identification code with an expired identification code; and

handling a communication addressed to the expired identification code according to instructions stored in the database and based on options previously set by the intended recipient.

21. The method of claim 7 wherein the instructions are based on the content of the communication.

22. The method of claim 7 including:

inserting a flag into a subsequent communication sent in reply to the communication, wherein the flag identifies the subsequent communication as a reply; and

automatically routing the subsequent communication to the sender based on the presence of the flag.

23. An article comprising a computer-readable medium including computer-executable instructions for causing a computer system to:

extract a first identification code from a communication, wherein the first identification code is associated with an intended recipient of the communication and is independent of a particular type of communication medium;

query a central database for directions regarding handling of the communication based on the identification code associated with the intended recipient, wherein the directions are based on options previously set by the intended recipient; and

handle the communication in accordance with the directions.

24. The article of claim 23 including instructions for causing the computer system to:

extract a second identification code from the communication, wherein the second identification code is associated with a sender of the communication and is independent of a particular type of communication medium, wherein the directions are based on both the first and second identification codes.

25. The article of claim 24 including instructions for causing the computer system to prevent delivery of the communication if the directions indicate that all communications addressed to the intended recipient from the sender are to be blocked.

26. The article of claim 23 including instructions for causing the computer system to store the content of an undelivered communication for a specified period to allow subsequent retrieval by the intended recipient.

27. The article of claim 23 including instructions for causing the computer system to reformat the communication for delivery over a specified medium and deliver the communication to the intended recipient via the specified medium, if the directions specify that communications addressed to the intended recipient from the sender are to be delivered over the specified medium.

28. The article of claim 24 including instructions for causing the computer system to automatically insert the second identification code into the communication in response to the entry of corresponding information by the sender.

29. The article of claim 23 including instructions for causing the computer system to:

detect communications that are broadcast;

store a list of identification codes of parties broadcasting messages; and

handle messages originating from a party on the list and addressed to the intended recipient in accordance with directions based on options previously set by the intended recipient with respect to messages originating from parties on the list.

30. The article of claim 23 including instructions for causing a computer system to:

extract a second identification code from the communication, wherein the second identification code is associated with a particular sender of the communication and is independent of a particular type of communication medium;

determine whether the intended recipient has previously set options indicating how communications from the particular sender are to be handled; and

handle the communication as having been sent by an unclassified sender if the intended recipient has not set options indicating how communications from the particular sender are to be handled.

31. The article of claim 30 including instructions for causing the computer system to handle the communication based on options previously set by the intended recipient for handling communications from unclassified senders.

32. The article of claim 23 including instructions for causing the computer system to automatically inform parties with whom the intended recipient has previously communicated about a new identification code selected by the intended recipient.

33. The article of claim 32 including instructions for causing the computer system to:

link the new identification code with an expired identification code; and

handle a communication addressed to the expired identification code according to directions stored in the database and based on options previously set by the intended recipient.

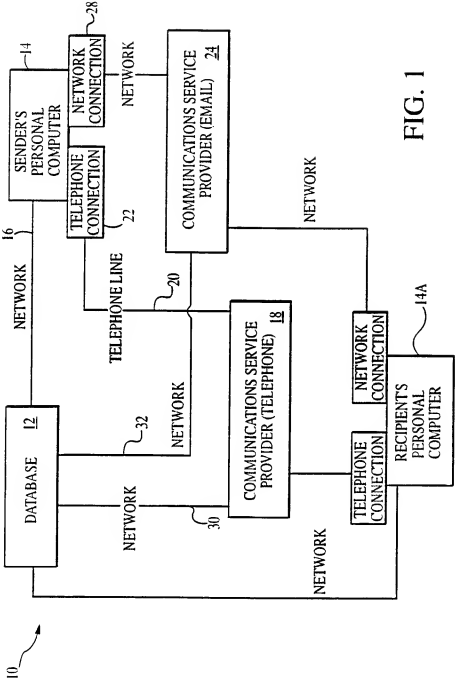

10
DATABASE 12
NETWORK
NETWORK
NETWORK
NETWORK
NETWORK
32
30
16
SENDER'S PERSONAL COMPUTER 14
TELEPHONE CONNECTION
NETWORK CONNECTION 28
TELEPHONE LINE
22
20
COMMUNICATIONS SERVICE PROVIDER (TELEPHONE) 18
COMMUNICATIONS SERVICE PROVIDER (EMAIL) 24
TELEPHONE CONNECTION
NETWORK CONNECTION
RECIPIENT'S PERSONAL COMPUTER
14A

FIG. 1

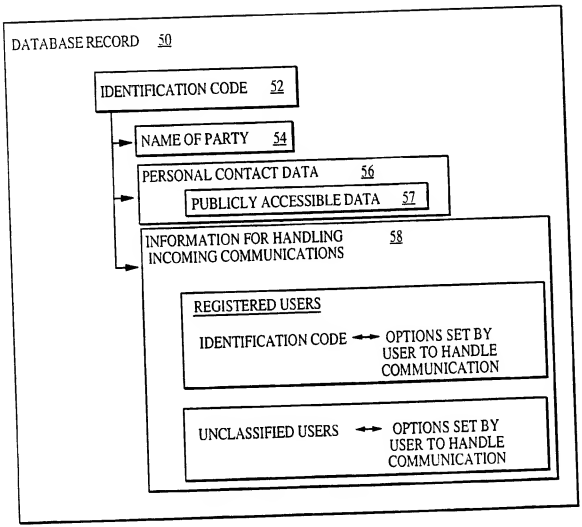

DATABASE RECORD 50
IDENTIFICATION CODE 52
NAME OF PARTY 54
PERSONAL CONTACT DATA 56
PUBLICLY ACCESSIBLE DATA 57
INFORMATION FOR HANDLING INCOMING COMMUNICATIONS 58
REGISTERED USERS
IDENTIFICATION CODE
OPTIONS SET BY USER TO HANDLE COMMUNICATION
UNCLASSIFIED USERS
OPTIONS SET BY USER TO HANDLE COMMUNICATION

FIG. 2

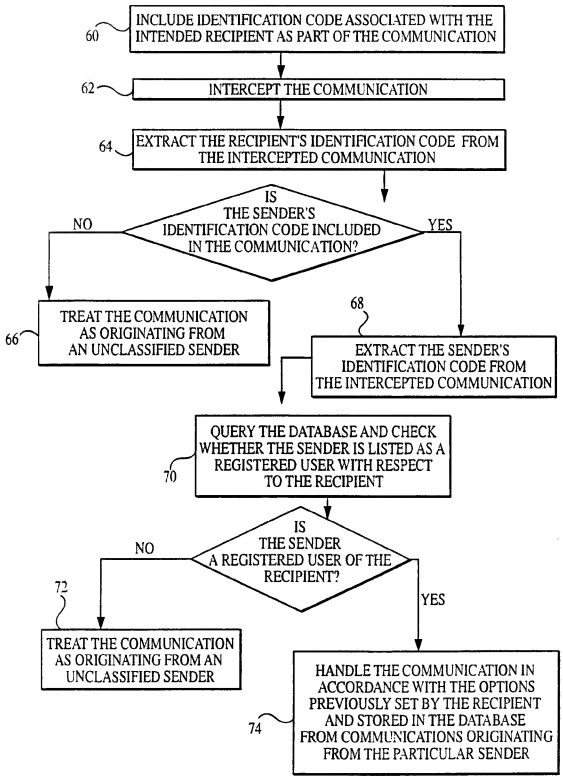

60
INCLUDE IDENTIFICATION CODE ASSOCIATED WITH THE INTENDED RECIPIENT AS PART OF THE COMMUNICATION
62
INTERCEPT THE COMMUNICATION
64
EXTRACT THE RECIPIENT'S IDENTIFICATION CODE FROM THE INTERCEPTED COMMUNICATION
IS THE SENDER'S IDENTIFICATION CODE INCLUDED IN THE COMMUNICATION?
NO
YES
66
TREAT THE COMMUNICATION AS ORIGINATING FROM AN UNCLASSIFIED SENDER
68
EXTRACT THE SENDER'S IDENTIFICATION CODE FROM THE INTERCEPTED COMMUNICATION
70
QUERY THE DATABASE AND CHECK WHETHER THE SENDER IS LISTED AS A REGISTERED USER WITH RESPECT TO THE RECIPIENT
IS THE SENDER A REGISTERED USER OF THE RECIPIENT?
NO
YES
72
TREAT THE COMMUNICATION AS ORIGINATING FROM AN UNCLASSIFIED SENDER
74
HANDLE THE COMMUNICATION IN ACCORDANCE WITH THE OPTIONS PREVIOUSLY SET BY THE RECIPIENT AND STORED IN THE DATABASE FROM COMMUNICATIONS ORIGINATING FROM THE PARTICULAR SENDER

FIG. 3

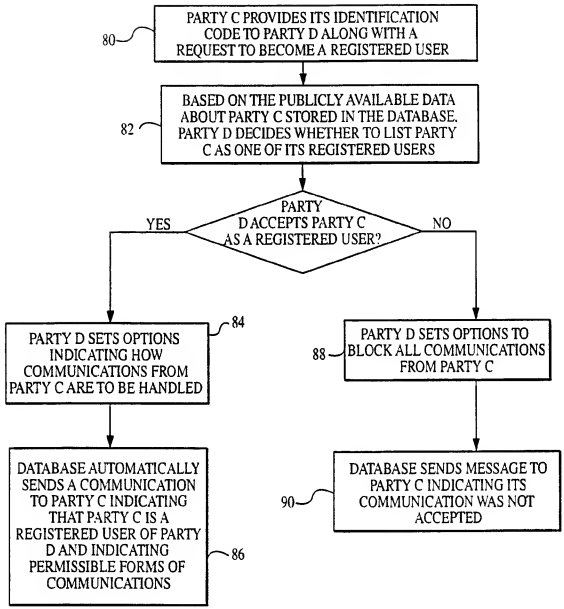

PARTY C PROVIDES ITS IDENTIFICATION CODE TO PARTY D ALONG WITH A REQUEST TO BECOME A REGISTERED USER
80
BASED ON THE PUBLICLY AVAILABLE DATA ABOUT PARTY C STORED IN THE DATABASE, PARTY D DECIDES WHETHER TO LIST PARTY C AS ONE OF ITS REGISTERED USERS
82
PARTY D ACCEPTS PARTY C AS A REGISTERED USER?
YES
NO
PARTY D SETS OPTIONS INDICATING HOW COMMUNICATIONS FROM PARTY C ARE TO BE HANDLED
84
PARTY D SETS OPTIONS TO BLOCK ALL COMMUNICATIONS FROM PARTY C
88
DATABASE AUTOMATICALLY SENDS A COMMUNICATION TO PARTY C INDICATING THAT PARTY C IS A REGISTERED USER OF PARTY D AND INDICATING PERMISSIBLE FORMS OF COMMUNICATIONS
86
DATABASE SENDS MESSAGE TO PARTY C INDICATING ITS COMMUNICATION WAS NOT ACCEPTED
90

FIG. 4

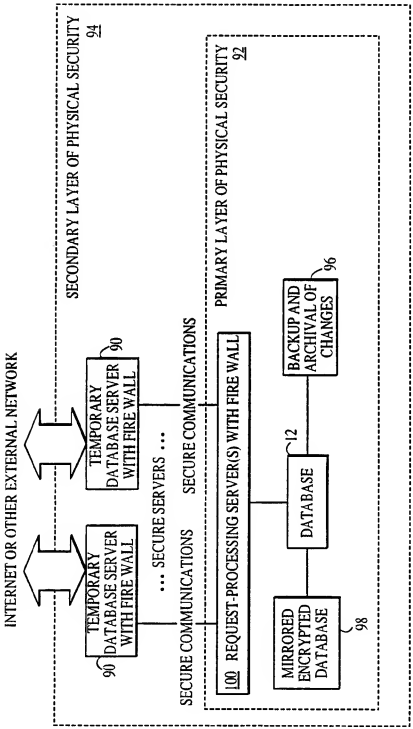

INTERNET OR OTHER EXTERNAL NETWORK
SECONDARY LAYER OF PHYSICAL SECURITY
94
TEMPORARY DATABASE SERVER WITH FIRE WALL
90
TEMPORARY DATABASE SERVER WITH FIRE WALL
90
... SECURE SERVERS ...
SECURE COMMUNICATIONS
SECURE COMMUNICATIONS
PRIMARY LAYER OF PHYSICAL SECURITY
92
100 REQUEST-PROCESSING SERVER(S) WITH FIRE WALL
MIRRORED ENCRYPTED DATABASE
98
DATABASE
12
BACKUP AND ARCHIVAL OF CHANGES
96

FIG. 5

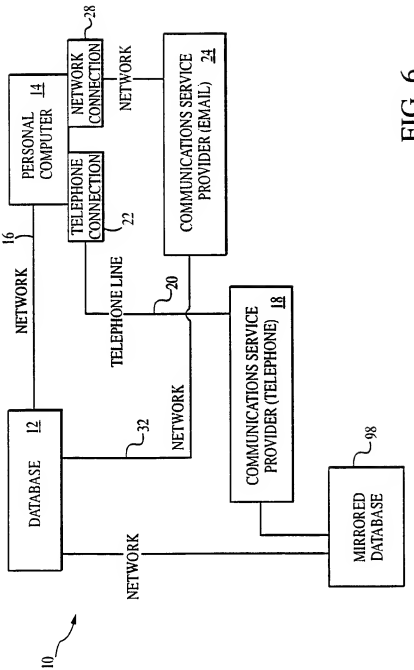

10
DATABASE 12
NETWORK 16
PERSONAL COMPUTER 14
TELEPHONE CONNECTION 22
NETWORK CONNECTION 28
NETWORK
TELEPHONE LINE 20
NETWORK 32
COMMUNICATIONS SERVICE PROVIDER (EMAIL) 24
COMMUNICATIONS SERVICE PROVIDER (TELEPHONE) 18
NETWORK
MIRRORED DATABASE 98

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/10606

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/30, 17/00
US CL. : 707/104, 10, 3

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/104, 10, 3

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,621,727 A (VAUDREUIL) 15 April 1997 (15.04.1997), ALL.	1-33
X	US 5,742,668 A (PEPE et al) 21 April 1998 (21.04.1998), ALL.	1-33

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2001 (28.06.2001)	02 AUG 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Uyen T Le Telephone No. 305-9000

Form PCT/ISA/210 (second sheet) (July 1998)